IN THE CLAIMS

Please amend claims 1, 17, 30 and 46 as follows:

1. (CURRENTLY AMENDED) A method for processing data comprising:

(a) performing an enrollment process, comprising:

receiving a first biometric data and a first personal key;

processing the first biometric data combined with the first personal key through an irreversible cryptographic algorithm to form a first processed data comprised of the first biometric data and the first personal key in an irreversibly encrypted form;

eliminating all storage or trace of the first biometric data and the first personal key in an unprocessed and unencrypted form after the first processed data has been formed and prior to any storage; and

storing the first processed data in a repository for use in a subsequent authentication process; and

(b) performing an authentication process, comprising:

receiving a second biometric data and a second personal key;

processing the second biometric data combined with the second personal key through the irreversible cryptographic algorithm to form a second processed data comprised of the second biometric data and the second personal key in an irreversibly encrypted form;

eliminating all storage or trace of the ~~first and~~ second biometric data and the second personal key [[s]] in an unprocessed and unencrypted form after the second processed data has been formed and prior to any comparison;

comparing the second processed data to the first processed data previously stored in the repository, without accessing either the first [[and]] or second processed data in an unprocessed and unencrypted form, in order to enable authentication of the ~~first and~~ second biometric data and the second personal key [[s]] in a confidential manner; and

generating a signal pertaining to the comparison of the second processed data to the first processed data for use in [[an]] the authentication process.

2. (ORIGINAL) The method of claim 1 further comprising generating a first variant from the first biometric data prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm.

3. (ORIGINAL) The method of claim 1 further comprising generating a second variant from the second biometric data prior to processing the second biometric data and the second personal key through the irreversible cryptographic algorithm.

4. (ORIGINAL) The method of claim 1 further comprising processing the first biometric data through a secondary irreversible cryptographic algorithm prior to processing the first biometric data and the second biometric data through the irreversible cryptographic algorithm.

5. (ORIGINAL) The method of claim 1 further comprising adding salt to the first biometric data and the first personal key.

6. (ORIGINAL) The method of claim 1 further comprising processing the first personal key through a cryptographic algorithm prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm.

7. (ORIGINAL) The method of claim 1 further comprising associating a first primary key to the first processed data.

8. (ORIGINAL) The method of claim 1 further comprising associating a second primary key to the second processed data.

9. (ORIGINAL) The method of claim 1 wherein receiving the first biometric data and the first personal key occurs during an enrollment process.

10. (ORIGINAL) The method of claim 1 wherein receiving the second biometric data and the second personal key occurs during an authentication process.

11. (ORIGINAL) The method of claim 1 wherein generating a signal includes issuing a confirmation signal when the second processed data matches the first processed data.

12. (ORIGINAL) The method of claim 11 wherein issuing a confirmation signal allows access to a facility.

13. (ORIGINAL) The method of claim 11 wherein issuing a confirmation signal allows access to a system.

14. (ORIGINAL) The method of claim 1 wherein generating a signal includes issuing a rejection signal when the second processed data does not match the first processed data.

15. (ORIGINAL) The method of claim 1 further comprising storing the first processed data in a database.

16. (ORIGINAL) The method of claim 15 wherein the database includes a plurality of first processed data.

17. (CURRENTLY AMENDED) A method for processing data comprising:

receiving biometric data and a personal key;

processing the biometric data combined with the personal key through an irreversible cryptographic algorithm to form a processed data comprised of the biometric data and the personal key in an irreversibly encrypted form;

eliminating all storage or trace of the biometric data and personal key in an unprocessed and unencrypted form prior to any comparison; and

comparing the processed data to secondary data stored in a repository, without accessing the processed data in an unprocessed and unencrypted form, in order to enable authentication of the biometric data and personal key in a confidential manner, wherein the secondary data comprises one or more combinations of biometric data and personal keys stored in the repository in an irreversibly encrypted form.

18. (ORIGINAL) The method of claim 17 further comprising generating a variant from the biometric data prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm.

19. (ORIGINAL) The method of claim 17 further comprising processing the biometric data through a secondary irreversible cryptographic algorithm prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm.

20. (ORIGINAL) The method of claim 17 further comprising adding salt to the biometric data and the personal key prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm.

21. (ORIGINAL) The method of claim 17 wherein receiving the biometric data and the personal key occurs during an authentication process.

22. (ORIGINAL) The method of claim 17 further comprising associating a primary key with the biometric data and the personal key.

23. (ORIGINAL) The method of claim 17 wherein the secondary data includes a secondary biometric data and a secondary personal key.

24. (ORIGINAL) The method of claim 23 wherein the secondary biometric data and the secondary personal key is received during an enrollment process.

25. (ORIGINAL) The method of claim 17 further comprising generating a signal corresponding to the comparison of the processed data to the secondary data.

26. (ORIGINAL) The method of claim 25 wherein generating a signal includes issuing a confirmation message when the processed data matches at least a portion of secondary data.

27. (ORIGINAL) The method of claim 25 wherein generating a signal includes issuing a denial message when the processed data does not match at least a portion of secondary data.

28. (ORIGINAL) The method of claim 25 wherein generating a signal allows entry into a facility when the processed data matches the secondary data.

29. (ORIGINAL) The method of claim 25 wherein generating a signal allows entry into a system when the processed data matches the secondary data.

30. (CURRENTLY AMENDED) A computer readable storage device storing program instructions for execution by a computer, such that when the computer executes the program instructions, it performs a method for processing data, comprising:

(a) performing an enrollment process, comprising:

receiving a first biometric data and a first personal key;

processing the first biometric data combined with the first personal key through an irreversible cryptographic algorithm to form a first processed data comprised of the first biometric data and the first personal key in an irreversibly encrypted form;

eliminating all storage or trace of the first biometric data and the first personal key in an unprocessed and unencrypted form after the first processed data has been formed and prior to any storage; and

storing the first processed data in a repository for use in a subsequent authentication process; and

(b) performing an authentication process, comprising:

receiving a second biometric data and a second personal key;

processing the second biometric data combined with the second personal key through the irreversible cryptographic algorithm to form a second processed data comprised of the second biometric data and the second personal key in an irreversibly encrypted form;

eliminating all storage or trace of the ~~first and~~ second biometric data and the second personal key [[s]] in an unprocessed and unencrypted form after the second processed data has been formed and prior to any comparison;

comparing the second processed data to the first processed data previously stored in the repository, without accessing either the first [[and]] or second processed data in an unprocessed and unencrypted form, in order to enable authentication of the ~~first and~~ second biometric data and the second personal key [[s]] in a confidential manner; and

generating a signal pertaining to the comparison of the second processed data to the first processed data for use in [[an]] the authentication process.

31. (ORIGINAL) The computer readable medium for performing the method of claim 30 further comprising generating a first variant from the first biometric data prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm.

32. (ORIGINAL) The computer readable medium for performing the method of claim 30 further comprising generating a second variant from the second biometric data prior to processing the second biometric data and the second personal key through the irreversible cryptographic algorithm.

33. (ORIGINAL) The computer readable medium for performing the method of claim 30 further comprising processing the first biometric data through a secondary irreversible cryptographic algorithm prior to processing the first biometric data and the second biometric data through the irreversible cryptographic algorithm.

34. (ORIGINAL) The computer readable medium for performing the method of claim 30 further comprising adding salt to the first biometric data and the first personal key prior to processing the first biometric data and the second biometric data through the irreversible cryptographic algorithm.

35. (ORIGINAL) The computer readable medium for performing the method of claim 30 further comprising processing the first personal key through a reversible cryptographic algorithm prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm.

36. (ORIGINAL) The computer readable medium for performing the method of claim 30 further comprising associating a first primary key to the first processed data.

37. (ORIGINAL) The computer readable medium for performing the method of claim 30 further comprising associating a second primary key to the second processed data.

38. (ORIGINAL) The computer readable medium for performing the method of claim 30 wherein receiving the first biometric data and the first personal key occurs during an enrollment process.

39. (ORIGINAL) The computer readable medium for performing the method of claim 30 wherein receiving the second biometric data and the second personal key occurs during an authentication process.

40. (ORIGINAL) The computer readable medium for performing the method of claim 30 wherein generating a signal includes issuing a confirmation signal when the second processed data matches the first processed data.

41. (ORIGINAL) The computer readable medium for performing the method of claim 40 wherein issuing a confirmation signal allows access to a facility.

42. (ORIGINAL) The computer readable medium for performing the method of claim 40 wherein issuing a confirmation signal allows access to a system.

43. (ORIGINAL) The computer readable medium for performing the method of claim 30 wherein generating a signal includes issuing a rejection signal when the second processed data does not match the first processed data.

44. (ORIGINAL) The computer readable medium for performing the method of claim 30 further comprising storing the first processed data in a database.

45. (ORIGINAL) The computer readable medium for performing the method of claim 44 wherein the database includes a plurality of first processed data.

46. (CURRENTLY AMENDED) A computer readable storage device storing program instructions for execution by a computer, such that when the computer executes the program instructions, it performs a method for processing data, comprising:

receiving biometric data and a personal key;

processing the biometric data combined with the personal key through an irreversible cryptographic algorithm to form a processed data comprised of the biometric data and the personal key in an irreversibly encrypted form;

eliminating all storage or trace of the biometric data and personal key in an unprocessed and unencrypted form prior to any comparison; and

comparing the processed data to secondary data stored in a repository, without accessing the processed data in an unprocessed and unencrypted form, in order to enable authentication of the biometric data and personal key in a confidential manner, wherein the secondary data comprises one or more combinations of biometric data and personal keys stored in the repository in an irreversibly encrypted form.

47. (ORIGINAL) The computer readable medium for performing the method of claim 46 further comprising generating a variant from the biometric data prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm.

48. (ORIGINAL) The computer readable medium for performing the method of claim 46 further comprising processing the biometric data through a secondary irreversible cryptographic

algorithm prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm.

49. (ORIGINAL) The computer readable medium for performing the method of claim 46 further comprising adding salt to the biometric data and the personal key prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm.

50. (ORIGINAL) The computer readable medium for performing the method of claim 46 wherein receiving the biometric data and the personal key occurs during an authentication process.

51. (ORIGINAL) The computer readable medium for performing the method of claim 46 further comprising associating a primary key with the biometric data and the personal key.

52. (ORIGINAL) The computer readable medium for performing the method of claim 46 wherein the secondary data includes a secondary biometric data and a secondary personal key.

53. (ORIGINAL) The computer readable medium for performing the method of claim 52 wherein the secondary biometric data and the secondary personal key is received during an enrollment process.

54. (ORIGINAL) The computer readable medium for performing the method of claim 46 further comprising generating a signal corresponding to the comparison of the processed data to the secondary data.

55. (ORIGINAL) The computer readable medium for performing the method of claim 54 wherein generating a signal includes issuing a confirmation message when the processed data matches at least a portion of secondary data.

56. (ORIGINAL) The computer readable medium for performing the method of claim 54 wherein generating a signal includes issuing a denial message when the processed data does not match at least a portion of secondary data.

57. (ORIGINAL) The computer readable medium for performing the method of claim 54 wherein generating a signal allows entry into a facility when the processed data matches the secondary data.

58. (ORIGINAL) The computer readable medium for performing the method of claim 54 wherein generating a signal allows entry into a system when the processed data matches the secondary data.